

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Appl. No.:	10/775,498	Confirmation No.	2317
Applicant:	GILMAN et al.	TC/A.U.:	2137
Filed:	February 9, 2004	Examiner	SMITHERS, M.
Docket No.:	4366-139		

For: "KEY SERVER FOR SECURING IP
TELEPHONY REGISTRATION,
CONTROL, AND MAINTENANCE"

Mail Stop Issue Fee
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

COMMENTS ON STATEMENT OF REASONS FOR ALLOWANCE

Dear Sir:

Applicant submits this Comments on Statement of Reasons for Allowance to address further the Notice of Allowability ("Notice") having a mailing date of November 11, 2007.

In the Notice, the Examiner's stated reasons for allowance were that "The present invention is directed to a method and system for providing secure communications between an application server and a packet-switched telecommunications device. Each independent claim identifies the uniquely distinct features of "providing, to the key generating agent through the session, when a key identifier is derived using the unique identifier associated with the first packet-switched communications device, the unique identifier when or when the key identifier is derived using information not associated with the first packet-switched communications device, no unique identifier when the receiving, from the key generating agent through the session, a secret key derived from an enterprise master key and a key identifier and the key identifier; forwarding to an application server a registration request, wherein the registration request comprises the key identifier and wherein the first packet-switched communications device has a limited ability to communicate with a provisioned and registered second packet-switched

communications device is successfully registered in step (g); authenticating the first packet-switched communications device with the secret key or an authentication key derived therefrom; and when the first packet-switched communications device, wherein steps (b) through (e) occur after the first packet-switched communications device has been located at an end user's premises and wherein the first and second packet-switched communications device have different and unique secret keys and key identifiers". Based on the Notice, the patentability of all other independent and dependent claims is assumed to be based upon the elements as set forth in such claims and that such claims meet all criteria for patentability under §101, §102, §103 and §112.

As is clear from MPEP 1302.14,

"The statement [of reasons for allowance] is not intended to necessarily state all the reasons for allowance or all the details why claims are allowed and should not be written to specifically or impliedly state that all the reasons for allowance are set forth."

While the above-stated may be a stated reason for allowing some independent claims, Applicant submits that some independent claims have a different reason for allowance and that some independent claims have other reasons for allowance.

Specifically, the prior art fails to teach the following features of Claims 1, 63, 82 and 99:

1. A method for provisioning and registering a packet-switched communications device in an enterprise network, comprising:

(a) providing an unprovisioned first packet-switched communications device in an enterprise network, the first packet-switched communications device having a corresponding unique identifier and an electronic address on the enterprise network;

(b) as part of a provisioning process establishing, by the first packet-switched communications device, a secure communications session with a key generating agent in the enterprise network;

(c) providing, to the key generating agent through the session, (i) when a key identifier is derived using the unique identifier associated with the first packet-switched communications device, the unique identifier or (ii) when the key identifier is derived using information not associated with the first packet-switched communications device, no unique identifier;

(d) receiving, from the key generating agent through the session, (i) a secret key derived from an enterprise master key and a key identifier and (ii) the

key identifier;

(e) forwarding to an application server a registration request, wherein the registration request comprises the key identifier and wherein the first packet-switched communications device has a limited ability to communicate with a provisioned and registered second packet-switched communications device in the enterprise network until the first packet-switched communications device is successfully registered in step (g);

(f) authenticating the first packet-switched communications device with the secret key or an authentication key derived therefrom; and

(g) when the first packet-switched communications device is successfully authenticated, registering the first packet-switched communications device, wherein steps (b) through (e) occur after the first packet-switched communications device has been located at an end user's premises and wherein the first and second packet-switched communications device have different and unique secret keys and key identifiers.

63. An enterprise network including a first packet-switched communications device having a corresponding unique identifier and an electronic address on the enterprise network, the first packet-switched communications device comprising:

a first processor in the packet-switched communications device operable to:

(A1) establish, as part of a provisioning process, a secure communications session with a key generating agent in the enterprise network;

(A2) provide, to the key generating agent through the session, (i) when a key identifier is derived using a unique identifier associated with the first packet-switched communications device, the unique identifier or (ii) when the key identifier is derived using information not associated with the first packet-switched communications device, no unique identifier;

(A3) receive, from the key generating agent through the session, (i) a secret key derived from a key identifier and an enterprise master key and (ii) the key identifier;

(A4) forward to an application server a registration request, wherein the registration request comprises the key identifier and wherein the first packet-switched communications device has a limited ability to communicate with a provisioned and registered second packet-switched communications device in the enterprise network until the first packet-switched communications device is successfully registered in operation (B2); and wherein the application server comprises a second processor that is operable to:

(B1) authenticate the communications device with the secret key or an authentication key derived therefrom; and

(B2) when the communications device is successfully authenticated,

register the communications device, wherein operations (A1) through (B1) occur after the first packet-switched communications device has been located at an end user's premises and wherein the first and second packet-switched communications device have different and unique secret keys and key identifiers.

82. A method for provisioning and registering a packet-switched communications device in an enterprise network, comprising:

- (a) assigning an electronic address to a first communications device;
- (b) providing the electronic address and an address associated with a key generating agent to the first communications device;
- (c) authenticating, by the first communications device, the key generating agent; and
- (d) when authentication of the key generating agent is successful, performing the following additional steps:
 - (e) establishing, as part of a provisioning process, a secure communications session between the first communications device and the key generating agent, wherein the first communications device has a corresponding unique identifier;
 - (f) providing the unique identifier to the key generating agent through the secure communications session;
 - (g) receiving, from the key generating agent through the session, (i) a secret key derived from an enterprise master key, the unique identifier, and a key identifier and (ii) the key identifier;
 - (h) forwarding to an application server a registration request, wherein the registration request comprises the key identifier and wherein the first communications device has a limited ability to communicate with a provisioned and registered second packet-switched communications device in the enterprise network until the first communications device is successfully registered in step (j);
 - (i) authenticating the first communications device with the secret key or an authentication key derived therefrom; and
 - (j) when the first communications device is successfully authenticated, registering the first communications device, wherein steps (e) through (j) occur after the first communications device has been located at an end user's premises and wherein the first and second packet-switched communications device have different and unique secret keys and key identifiers.

99. A method, comprising:

- (a) requesting, by an unprovisioned and unregistered first communications device, a first electronic address to be assigned to the first communications device and a second electronic address associated with a key generating agent;
- (b) receiving, by the first communication device, the first and second electronic addresses;

- (c) thereafter contacting and authenticating, by the first communications device, the key generating agent;
- (d) when authentication of the key generating agent is successful, establishing, by the first communications device and as part of a provisioning process, a secure communications session with the key generating agent, wherein the first communications device has a corresponding unique identifier;
- (e) providing the unique identifier to the key generating agent through the secure communications session;
- (g) receiving, from the key generating agent through the session, a secret key derived from an enterprise master key, the unique identifier, and a key identifier;
- (h) forwarding, to an application server, a registration request, wherein the registration request comprises the key identifier and wherein the unregistered first communications device has a limited ability to communicate with a provisioned and registered second packet-switched communications device in the enterprise network until the first communications device is successfully registered; and
- (i) when the application server, has successfully authenticated the first communications device using the secret key or an authentication key derived therefrom, registering the first communications device, wherein steps (a) through (i) occur after the first communications device has been located at an end user's premises and wherein the first and second packet-switched communications devices have different and unique secret keys and key identifiers.

Although the Applicant believes that no fees are due for filing this Comments on Statement of Reasons for Allowance, please charge any fees deemed necessary to Deposit Account No. 19-1970.

Respectfully submitted,

SHERIDAN ROSS P.C.

By: 

Douglas W. Swartz
Registration No. 37,739
1560 Broadway, Suite 1200
Denver, Colorado 80202-5141
(303) 863-9700

Date: Nov 27, 2007